of security tags associated with the superset or pages of the report; and

associating a value with each one of the first plurality of complete cells ~~complete cell~~ based on whether the user can view a particular page.

Please **ADD** new claims as follows:

35.   (New) A method as recited in claim 1, wherein a data break is a level break in the data.

36.   (New) A method as recited in claim 1, wherein the security information comprises one or more database fields.

37.   (New) A method as recited in claim 1, wherein the security information comprises information indicating one or more levels of access to the data.

REMARKS

In the Office Action, the Examiner rejected the claims under 35 USC §103. The claims have been amended to further clarify the subject matter regarded as the invention. In addition, claims 35-37 have been added. Claims 1-37 are now pending. The rejections to the claims are fully traversed below.

Reconsideration of the application is respectfully requested based on the following remarks in view of the amended claims.

REJECTION OF CLAIMS UNDER 35 USC §103

Independent claims 1 and 28

In the Office Action, the Examiner rejected claims 1, 2, 3, 8, 9, 28 and 29 under 35 USC §103 as being unpatentable over McIntosh, U.S. Patent No. 6,185,576, ('McIntosh' hereinafter), Shisler et al, U.S. Patent No. 2001/0018708, ('Shisler' hereinafter), and Nessett

et al, U.S. Patent No. 5,727,143, ('Nessett' hereinafter). This rejection is fully traversed below.

The invention as recited in claim 1, as amended, creates a report. The report created includes <u>security tags associated with pages of the report</u>. In this manner, the invention as recited in claim 1, as amended, enables <u>page-level security</u> to be implemented. None of the references, separately or in combination, enable page-level security to be implemented.

McIntosh discloses a uniform subject classification system. See Title. Specifically, McIntosh discloses an interlingual mechanism to achieve uniformity when classifying anything by subject. Using generic terminology in a hierarchical structure, it directs the user to a single classification. The system captures terms into a thesaurus that can be modified and appended as classification needs change. The system "learns" as synonyms are added to "family groups", capturing differences in individual perception. In addition, the system may be searched by entering a descriptive term, which results in information pertaining to the item. See Abstract. As the Examiner recognizes, <u>McIntosh does not teach or suggest the use the use of security tags in the manner claimed</u>. For instance, McIntosh neither discloses nor suggests "retrieving a data row <u>and associated security information from a data source, the data row</u> having data to be contained in the report," "forming a first security tag <u>from the security information that has been retrieved from the data source</u> if the data row causes a data break," "associating the first security tag with a new page in the report wherein the data row is placed on the new page <u>such that security is implemented at the page level for the new page in the report</u>," or "placing subsequent data rows on pages having the first security tag <u>associated therewith</u> until a second security tag is formed such that data in the report is organized based on a plurality of security tags <u>such that security is implemented at the page level for the pages associated with the plurality of security tags</u>," as recited in claim 1, as amended. For instance, the security information may include one or more security identifiers, as recited in claim 3.

The Examiner seeks to cure the deficiencies of McIntosh with Shisler and Nessett. Specifically, Shisler discloses a data processing system that includes client and server computers of various platform types, interconnected by a network. A batch processing engine permits an application resident on a client computer to specify processing to be performed by one or more of the computers connected to the network, regardless of the platform type of such computers. See Abstract. During batch processing, a check is made to

determine whether the current level being processed is at a data break. If not, processing returns to fetch another level break specification. If the current level being processed is determined to be at a data break, child processing takes place. See p. 8, par. 0112. Thus, Shisler appears to disclose a standard batch processing engine.

Nessett discloses a mechanism for locating objects. See Title. In a distributed object computing system, the client makes a call to a daemon process of a host computer in order to communicate with a target object in an object server process. This call uses a particular security mechanism to ensure a secure communication. The daemon process locates the object server and starts it if necessary. The object server provides the daemon process with a list or table of all the particular security mechanisms that it supports. Using a security class identifier provided by the client in the original call, the daemon process selects a particular security mechanism supported by the server, and then returns this new security mechanism along with the server's port to the client. See Abstract.

The security information list in Nessett is described in one embodiment as implemented as a sequence of Tagged Components. Each Tagged Component includes a Tag and Component Data associated with that Tag. Component Data is associated with each Tag. The Component Data defines for each security mechanism identified by the corresponding Tag the services that the mechanism allows a target object to require or allows a target object to support. Depending upon the security mechanism identified by the Tag, the Component Data may include other information needed to implement that security mechanism. See col. 10, line 58 – col. 11, line 35. Nessett further discloses an object reference that includes an object server identifier, original security information, and a security class identifier. See col. 2, lines 28-30.

As set forth above, Nessett discloses a security information list in which each tagged component includes a tag, which identifies a security mechanism. The security information list merely lists security mechanisms supported by the server. Therefore, this list is static rather than dynamic. The cited references neither disclose nor suggest associating security tags with data (e.g., pages in a report). Rather, the security mechanisms in the security information list of Nessett are independent from the context in which the server will use them (e.g., independent from data that may be transmitted). Accordingly, Nessett teaches away from the present invention.

The cited references, separately or in combination, neither disclose nor suggest associating a security tag with a new page in a report wherein the data row is placed on the new page. Moreover, the cited references, separately or in combination, fail to disclose or suggest placing subsequent data rows on pages having the first data tag until a second security tag is formed such that data in the report is organized based on a plurality of security tags. Similarly, the cited references fail to disclose or suggest comparing security information associated with a user with such security tags in order to ascertain which pages of a report are viewable by the user (e.g., claims 10 and 11).

Since the cited references together fail to disclose each of the claimed elements, the combination of these references also fails to disclose or suggest the claimed invention. Moreover, since the cited references together fail to disclose each of the claimed elements, the combination of the references would fail to achieve the desired result. In addition, it is important to note that there is no motivation to combine the above-cited references. Accordingly, Applicant respectfully submits that independent claims 1 and 28 are patentable over the cited art.

Independent claims 12 and 32

In the Office Action, the Examiner rejected claims 12, 13, 23-25, and 32 under 35 USC §103 as being unpatentable over McIntosh, Nessett, and Jebens, U.S. Patent No. 6,332,145, ('Jebens' hereinafter). This rejection is fully traversed below.

The Examiner admits that McIntosh does not teach the use of security tags, security identifiers or allowing users to view only the data they are authorized to view. The Examiner seeks to cure the deficiencies of McIntosh with Nessett and Jebens. However, as described above with reference to claims 1 and 28, Nessett neither discloses nor suggests associating security tags with data or pages within a report. Moreover, Nessett neither discloses nor suggests retrieving a report having a superset of pages, a page from the superset of pages having a security tag. While Jebens indicates that reports may only be viewed by an authorized user (col. 13, lines 6-7), Jebens fails to cure the deficiencies of McIntosh and Nessett. In other words, Jebens fails to disclose or suggest associating security tag with a page in a report or, alternatively, retrieving a page in a report based upon an associated security tag. It is also important to note that Jebens implies that an authorized user may view entire reports, rather than specific portions (or pages) within a report. As a result, Jebens

teaches away from securing individual pages with associated security tags. Thus, the cited references, separately or in combination, fail to disclose or suggest "retrieving a report having a superset of pages, a page one or more pages from the superset of pages having a security tag associated therewith such that a plurality of security tags are associated with the superset of pages of the report," "obtaining a list of security identifiers associated with the user," "comparing the list of security identifiers associated with the user with a the plurality of security tags associated with the superset of pages of the report," and "deriving a subset of pages from the superset of pages based on the comparison such that the subset of pages only contains data that the user is authorized to view" as recited in claim 12, as amended. Accordingly, Applicant respectfully submits that claims 12 and 32 are patentable over the cited references.

The dependent claims depend from one of independent claims 1, 12, 28, and 32 and are therefore patentable for at least the same reasons. However, the dependent claims recite additional limitations that further distinguish them from the cited references. Hence, it is submitted that the dependent claims are patentable over the cited art.

Based on the foregoing, it is submitted that claims 1, 12, 28, and 32 are patentably distinct from the cited references. In addition, it is submitted that the dependent claims are also patentable for at least the same reasons. The additional limitations recited in the independent claims or the dependent claims are not further discussed as the above discussed limitations are clearly sufficient to distinguish the claimed invention from the cited references. Thus, it is respectfully requested that the Examiner withdraw the rejection of the claims under 35 USC §103(a).

SUMMARY

Reconsideration of the application and an early Notice of Allowance are earnestly solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned attorney at the telephone number listed below.

Applicants hereby petition for an extension of time which may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 50-0388 (Order No. ACTUP002).

Respectfully submitted,
BEYER, WEAVER & THOMAS , LLP

Elise R. Heilbrunn
Reg. No. 42,649

BEYER, WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778
Tel. (510) 843-6200